IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA	§	
	§	
v.	§	
	§	No.
THOMAS JAMES FREDERICK SMITH (1)	§	
also known as Zook, TJ, and kingsmith007	§	3-09CR 100-B
DAVID ANTHONY EDWARDS (2)	§	
also known as DAVUS	§	

INDICTMENT

The Grand Jury Charges:

INTRODUCTION

At all times material to this indictment, or as otherwise specified,

1. **Thomas James Frederick Smith, also known as Zook, TJ, and kingsmith007,** lived in Nebraska.

2. **Smith** was the administrator for the domain z00k.us.

3. **Smith** maintained and used the following email accounts; kingsmith007@yahoo.com; kingsmith007@hotmail.com; z00kus@gmail.com; and kingsmith_007@hotmail.com.

4. **David Anthony Edwards, also known as Davus,** lived in Mesquite, Texas, in the Northern District of Texas, Dallas Division.

5. **Edwards** maintained a server at his home, and operated the website Kidindustries.net from at least August 2004 through October 2007.

6. On Kidindustries.net, **Edwards** hosted an Internet Relay Chat site, published his own blog, and provided links to other sites, including z00k.us.

7. **Smith** maintained z00k.us on the server located in **Edwards**' residence.

8. CCpowerForums.com was a website that hosted user forums entitled "hacking," "exploits," "proxies," "trojans/keyloggers/bots, credit cards," and "hall of shame."

9. T35.net provided free and paid personal and business web hosting services for hundreds of thousands of users.

10. ThePlanet.com was an internet hosting company located in the Northern District of Texas, Dallas Division. ThePlanet.com provided its customers with large scale Internet connectivity, access to networks of computers, and the use of servers and other hardware.

11. Icegold (IceGold.com) was a digital currency exchanger which operated from at least January 2001 through at least January 2008.

E-Gold (e-gold.com) is an Internet based account, dealing in electronic currency, issued by e-gold Ltd., a Nevis corporation, 100% backed at all times by gold bullion in allocated storage.

Definitions

12. Internet Relay Chat (IRC) is a form of real-time Internet text messaging (chat) or synchronous conferencing. It is mainly designed for group communication in discussion

forums, called channels, but also allows one-to-one communication via private message, as well as chat and data transfers via direct client-to-client. A client is a computer, or software running on that computer, that is used by a person to chat through IRC. A server is a centralized computer that manages connections between the many clients and relays messages to the appropriate recipients. IRC offers the ability to have private conversations with only select clients or public conversations with only select clients or public conversations with multiple clients. IRC uses "channels" to determine which users are parties to which conversations. IRC supports the use of passwords, or "keys" to limit access to servers and channels. IRC also provides an administrative level of access, known as an "operator," at the channel and server level to provide configuration and policy enforcement. IRC channels have names, that uniquely identify them, and "topics," that usually describe the conversation happening on the channel.

13. An IRC network is a collection of computers communicating with each other through IRC. Generally, an IRC network includes numerous clients (between a few dozen and tens of thousands) and one or several servers (most small networks can operate with only one server, but many have several for performance and availability reasons). Servers are generally always available, while clients connect and disconnect at various times.

14. An IRC robot, or "bot," is a program running on an IRC client that responds automatically to commands sent to it by the IRC server. The bot can thus receive commands, perform functions, and provide information back to the IRC server without human interaction at the client level. A computer infected with a malicious IRC bot and connected to an IRC server can be controlled by the operator of the bot.

15. An IRC botnet is large number of computers infected with bots. The infected computers are configured to connect to an IRC channel and "wait" there for further commands. The botnet operator or controller (i.e., a human using an IRC client program) issues those commands by connecting to the IRC server, on the appropriate channel, and then issuing the commands. Many malicious bot programs are also capable of interpreting an IRC channel topic as a command. This allows the owner/operator of the botnet to configure a persistent command, which will be received and executed by every infected computer as it connects to the channel. This allows the botnet to operate without constant interaction by the operator of the network.

16. Malicious bots are installed on computers without the knowledge or consent of the computers' owners. The creator of the bot program typically does this by using a computer or computers to electronically scan or search the Internet for computers with particular vulnerabilities or security weaknesses. The bot creator then uses an "exploit" or computer code written to take advantage of those vulnerabilities or weaknesses to compromise or "hack" the victim computer. Once the victim computer has been hacked,

the computer can be infected through the installation of malicious bot program. The bot program causes the infected computer to connect to the appropriate IRC channel, where it will receive commands through program codes from the operator of the botnet.

17. A "distributed denial of service attack," or "DDOS attack" is a type of malicious computer activity in which an attacker directs a large number of infected computers to simultaneously and repeatedly "flood" a victim computer with large amounts of data or specified computer commands. A DDOS attack typically renders the victim computer unable to handle legitimate network traffic and often the victim computer will be unable to perform its intended function and legitimate users are denied the services of the computer. Depending on the type and intensity of the DDOS attack, the victim computer and its network may become completely disabled, causing loss to persons who use the victim computer. Further, it can take significant time, expertise, and expense to respond to and defend against a DDOS attack.

18. "Flooding" means to upload a huge amount of data or engage in repeated actions in order to saturate the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

19. A "keylogger" is a program or device that when installed on a computer, records the keystrokes entered on that computer. Those keystrokes can then be accessed at a later date to see what the users have typed on that machine.

20. "Exe" is short for "executable" or ".exe" or executable file, and refers to a binary file containing a program that is ready to be executed or run by a computer.

21. "Carding" is the theft and unauthorized use of credit and debit card and other financial information.

22. "Hacking" is defined as illegally breaking into computers and network systems by exploiting vulnerabilities in those systems.

COUNT ONE

Conspiracy to Intentionally Cause Damage to a Protected Computer
and to Commit Computer Fraud
(18 U.S.C. §371)
(18 U.S.C. §§1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and §1030(a)(6)(A))

1. The grand jury realleges and incorporates the Introduction and Definitions sections of the Indictment.

2. Beginning in or about the summer of 2004 and continuing through October 2006, in the Dallas Division of the Northern District of Texas and elsewhere, defendants **Thomas James Frederick Smith, also known as Zook, TJ, and kingsmith007,** and **David Anthony Edwards, also known as Davus**, did knowingly and willfully conspire, combine, confederate, and agree with each other and with others known and unknown to the Grand Jury to commit offenses against the United States, to wit:

a. to cause the transmission of a program, information, code, or command through the use of an Internet Relay Chat network, and as a result of such conduct, cause damage without authorization to a protected computer producing an aggregate loss of at least $5,000.00 within a twelve month period, in violation of 18 U.S.C. §§1030(a)(5)(A)(i) and 1030(a)(5)(B)(i); and

b. to traffic in and affecting interstate commerce, in any password or similar information through which a computer may be accessed without authorization, in violation of 18 U.S.C. §1030(a)(6)(A);

OVERT ACTS:

3. In furtherance of the conspiracy and to accomplish its objects, **Thomas James Frederick Smith, also known as Zook, TJ, and kingsmith007,** and **David Anthony Edwards, also known as Davus**, and others known and unknown to the Grand Jury, committed the following overt acts, among others in the Dallas Division of the Northern District of Texas and elsewhere:

a. On or about June 10, 2004, **Smith** joined CCpowerForums.com using the alias "Zook." **Smith** identified his personal home page as www.z00k.us, and noted that he could be contacted through the instant messaging services at kingsmith007@hotmail.com.

b. On or about June 11, 2004, **Smith** posted a message to the Miscellaneous forum at CCpowerForums.com in which he identified himself as Zook and kingsmith007. **Smith** also stated that he had "been in the warez business for about 3 years" and had previously participated in hacking and carding.

c. In or before January 2005, **Edwards** created or developed a bot called NETTICK, a coded application that could be used to infect multiple computers to create a botnet. From at least January 2005 through October 2006, **Edwards** and **Smith** worked together over the Internet to further develop the NETTICK bot.

d. On or about January 17, 2005, **Smith** accessed CCpowerForums.com and sent a private message to another CCpowerForums member describing his bot as a DDoS bot with flooding features. **Smith** stated that he and another person created the bot and possessed the source code to control or command the infected computers.

e. On or about February 2, 2005, **Smith** accessed CCpowerForums.com and sent a private message to another member stating that he was continuing to update or improve the source code for the privately developed bot.

f. From at least the spring of 2005 and continuing through October 2006, **Edwards** and **Smith** were "operators" on the IRC forum on Kidindustries.net. Between the spring of 2005 and continuing through October 2006, **Edwards** and **Smith** used irc.Kidindustries.net to operate and command the infected computers.

g. On or about April 10, 2005, a NETTICK coded application file was created on an infected computer in Milan, Tennessee (the infected Milan computer). The NETTICK coded application file was last accessed on the infected Milan computer on or about October 20, 2006.

h. In or about April 2005, a NETTICK coded application file was created on a computer in Mesquite, Texas (the infected Mesquite computer). The NETTICK coded application file was last accessed on the infected Mesquite computer in or after October 2006.

i. Between the spring of 2005 and October 2006, **Edwards** and **Smith** commanded and controlled numerous computers (a botnet) infected with the NETTICK bot, including the infected Milan and Mesquite computers.

j. On or about February 4, 2006, a NETTICK bot logged into Kidindustries.net from an Internet Protocol address belonging to the infected Milan computer.

k. On or about July 27, 2006, **Smith** posted a public message, subject "Hybrid Bot", in which he offered to sell the executable program to control the botnet for $750 or source code for $1,200.

l. On or about October 14, 2006, **Smith** sent an email from kingsmith007@yahoo.com to a potential botnet purchaser, claiming to have 21,892 infected computers on 3 servers. Smith offered to sell the infected computers for 15 cents each, but required a minimum purchase of 5000. Smith also offered to sell the bot source code only if the purchaser bought the entire botnet.

m. On or about August 14, 2006, **Smith** demonstrated the bot's capabilities and caused a portion of the botnet, including the infected Milan and Mesquite computers, to engage in a DDOS attack by flooding an IP address at ThePlanet.com. **Smith** admitted that demonstration involved only a limited portion of his botnet. After the test, the bot purchaser agreed to buy the source code and the entire botnet for approximately $3,000, with a $1,500 downpayment. **Smith** conducted the demonstrative DDOS attack through commands given to the infected computers at irc.Kidindustries.net.

n. On or about August 15, 2006, **Smith** directed the bot purchaser to transfer approximately $1,600 into an E-Gold account number 2880161. Smith caused the downpayment to be transferred to an IceGold E-Gold account #372. On August 21, 2006, **Smith** caused a wire transfer from MR's IceGold E-Gold account #372 to **Smith**'s First State Bank checking account, which account number ended in 898.

o. On or about September 26, 2006, **Smith** and **Edwards** accessed without authorization the T35.net database, containing user identifications and passwords.

p. On or about September 26, 2006, **Smith** and **Edwards** extracted shadow password files from the T35.net database, and using a conventional password cracking tool, gained access to the passwords.

q. On or about September 26, 2006, **Smith** and **Edwards** downloaded T35.net's user database containing hundreds of thousands of user identifications and passwords.

r. On or about October 3, 2006, **Smith** and **Edwards** defaced the T35.net website, and made public the user identifications and passwords.

s. On or about October 4, 2006, **Smith** posted a message on HelpingWebmasters.com to advise T35.net's administrator that the T35.net website had been defaced and its user database compromised. **Smith** asked the administrator, "How are all the users going to be compensated?"

t. From in or about 2005, and continuing through in or about October 2006, **Edwards** possessed various versions of the NETTICK executable program on the server in his home, archived in the file home.tar.

In violation of 18 U.S.C. §371 (18 U.S.C. §§1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and §1030(a)(6)(A)).

A TRUE BILL:

FOREPERSON

JAMES T. JACKS
ACTING UNITED STATES ATTORNEY

CANDINA S. HEATH
Assistant United States Attorney
State of Texas Bar No. 09347450
1100 Commerce Street, 3rd Floor
Dallas, Texas 75242
Telephone: 214.659.8600
candina.heath@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA

v.

THOMAS JAMES FREDERICK SMITH (1)
also known as zOOK, TJ, and kingsmith
DAVID ANTHONY EDWARDS (2)
also known as DAVUS

3-09CR 100-B

INDICTMENT

18 U.S.C. § 371 (18 U.S.C. §§ 1030(a)(5)(A)(i),
1030(a)(5)(B)(i) and § 1030(a)(6)(A)
Conspiracy to Intentionally Cause Damage to a Protected Computer
and to Commit Computer Fraud

1 Count

A true bill rendered:

DALLAS FOREPERSON

Filed in open court this 8th day of April, A.D. 2009.

Clerk

PLEASE ISSUE ARREST WARRANT for THOMAS JAMES FREDERICK SMITH and DAVID ANTHONY EDWARDS

Jorge A. Solis

UNITED STATES DISTRICT/~~MAGISTRATE JUDGE~~

Magistrate Case No. 3:06-MJ-431
No Pending Criminal Complaint

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS

Related Case Information

Superseding Indictment: □ Yes ☒ No New Defendant: ☒ Yes □ No

Pending CR Case in NDTX: □ Yes ☒ No If Yes, number:

Search Warrant Case Number N/A

R 20 from District of N/A

Magistrate Case Number: N/A

1. **Defendant Information**

Juvenile: □ Yes ☒ No

If Yes, Matter to be sealed:

□ Yes ☒ No

Defendant Name THOMAS JAMES FREDERICK SMITH (1)

Alias Name a/k/a zOOk, TJ, and kingsmith

Address

County in which offense was committed: Dallas

2. **U.S. Attorney Information**

Candina S. Heath Bar # 09347450

3. **Interpreter**

□ Yes ☒ No If Yes, list language and/or dialect:

4. **Location Status**

Arrest Date: Issue arrest warrant

□ Already in Federal Custody
□ Already in State Custody
□ On Pretrial Release

5. **U.S.C. Citations**

Total # of Counts as to This Defendant: 1 □ Petty □ Misdemeanor ☒ Felony

Citation	Description of Offense Charged	Count(s)
18 U.S.C. § 371 (18 U.S. C. §§ 1030(a)(5)(A)(i), § 1030(a)(5)(B)(i) and § 1030(a)(6)(A)	Conspiracy to Intentionally Cause Damage to a Protected Computer & to Commit Computer Fraud	1

Date 4-3-09 Signature of AUSA:

Criminal Case Cover Sheet 3-09CR-100-B Revised 3/5/98

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS

Related Case Information

Superseding Indictment: □ Yes ☒ No New Defendant: ☒ Yes □ No

Pending CR Case in NDTX: □ Yes ☒ No If Yes, number:

Search Warrant Case Number 3:06-MJ-431

R 20 from District of N/A

Magistrate Case Number: 3:06-MJ-431

1. **Defendant Information**

Juvenile: □ Yes ☒ No

If Yes, Matter to be sealed:

□ Yes ☒ No

Defendant Name DAVID ANTHONY EDWARDS (2)

Alias Name a/k/a DAVUS

Address

County in which offense was committed: Dallas

2. **U.S. Attorney Information**

Candina S. Heath Bar # 09347450

3. **Interpreter**

□ Yes ☒ No If Yes, list language and/or dialect:

4. **Location Status**

Arrest Date: Issue arrest warrant

□ Already in Federal Custody
□ Already in State Custody
□ On Pretrial Release

5. **U.S.C. Citations**

Total # of Counts as to This Defendant: 1 □ Petty □ Misdemeanor ☒ Felony

Citation	**Description of Offense Charged**	**Count(s)**
18 U.S.C. § 371 (18 U.S. C. §§ 1030(a)(5)(A)(i), § 1030(a)(5)(B)(i) and § 1030(a)(6)(A)	Conspiracy to Intentionally Cause Damage to a Protected Computer & to Commit Computer Fraud	1

Date 4-3-09 Signature of AUSA: